**IT Applications, Unit 4**

**Security and ethical considerations, Ch 8, p 294**

Security Equipment

**Security Software**

Describe each of the following software-based security types.

1. Encryption software

Encryption software is where a message is encrypted by the use of an algorithm.

* 1. What are the two types of modern encryption methods?
     + Symmetric-key encryption
     + Asymmetric-key encryption

1. Network policies, profiles

Its there so that when the employee enters a username and password to logon to the networked system. They are then matched against the various resources they have permission to access.

1. Firewalls

They are used to restrict access to outsiders to a network, as well as protect personal information, such as payrolls and personal records, from employees not authorised to access it.

1. Antivirus software

Antivirus software detects the presence of viruses as the computer boots up, when a executable file is run, when documents are accessed or when files are copied.

**Security Procedures, p 299**

**Communication:**

1. List the security considerations for communication within an organisation.

* Well documented processes for communicating sensitive information via email, telephone and fax.
* Use of passwords on documents that have sensitive information.
* Well documented policy for the use of networked devices within the organisation.

**Storage**

1. **Filenaming conventions**
   1. List the 3 types of information each document should include.

* Date stamp
* Variation
* Name
  1. Give an example of a sequential file-naming convention.

‘newsletter 2011-11 03Oct. doc’. This is a monthly newsletter. The edition being prepared is for November 2011. The revision was saved on 3 October and is named sequentially.

1. **Location of files**
2. **Backups**
   1. Distinguish between each of the following:
      1. Full backup

Where it copies all of the files from a device to a storage medium.

* + 1. Differential backup

Where it copies only those files that have been changed since the last full backup.

* + 1. Incremental backup

It is similar to a differential backup but it uses more than two media backup media.

1. **Backup timeline**
   1. List good practice in relation to backup timelines.

* Clearly label all backup media
* Keep a log on recording backup dates
* Keep a log on the location of backup files
* Also keep a log on any restorations that have been made.

1. **Location of backup files**
   1. List good practice in the relation to the storage of backup files.

* Store in a location that is safe from theft and damaged caused by extreme temperatures or disaster.
* If possible store backups in a remote location like another city.
  1. What is the grandparent-parent-child system?

It is a backup routine, where the parent is the second oldest copy of the file and the child is the most recent copy of the file. An incremental backup is performed each day, with a differential backup at the end of week and a full backup at the end of each month.

1. **Archiving and destruction**
   1. Distinguish between archiving and destruction?

Archiving is essentially a process of copying files to long term storage, then deleting them from the hard disk.

Destruction involves deletion only.

* 1. What is a problem for ICT managers?

A problem is determining which is the most appropriate long term storage medium to use.

* 1. What is a legacy system?

It is a system that might run old databases on old servers or mainframes.

1. **Disposal**
   1. What issues must organisations consider in disposing information?

They must consider the protecting of sensitive data.